Install nFsen Netflow Analyzer on CENTOS 7

Configure Selinux

Configure SELinux in permissive mode:

```
# sed -i 's/SELINUX=.*/SELINUX=permissive/g' /etc/selinux/config
# setenforce 0
```

Install and Configure Nfsen:

It need to install a number of packages to get NFSEN running:

```
# yum install httpd php wget gcc make rrdtool-devel rrdtool-perl perl-MailTools perl-
  Socket6 flex byacc perl-Sys-Syslog perl-Data-Dumper
```

```
# yum install -y autoconf automake httpd php perl-MailTools rrdtool-perl perl-Socket6
  perl-Sys-Syslog.x86_64 policycoreutils-python tcpdump
```

```
# echo "date.timezone = Asia/Dhaka" > /etc/php.d/timezone.ini
```

Create the netflow user account and add it to the apache group:

```
# useradd netflow -G apache
```

Create the directories for nfsen and nfsen web:

```
mkdir -p /data/nfsen
mkdir -p /var/www/html/nfsen
```

Download the latest nfdump and nfsen packages. At time of this writing the latest versions are nfdump-1.6.13.tar.gz and nfsen-1.3.8.tar.gz

```
# cd /opt/
# wget http://downloads.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
# wget https://github.com/p-alik/nfsen/archive/refs/tags/nfsen-1.3.8.tar.gz
```

Install Nfdump

Untar the downloaded nfdump package into the "/opt/" Directory.

```
# cd /opt
# tar -zxvf nfdump-1.6.13.tar.gz
```

Compile nfdump while in the "/opt/nfdump-1.6.13" directory:

```
# cd /opt/nfdump-1.6.13
# ./configure --prefix=/opt/nfdump --enable-nfprofile --enable-nftrack --enable-sflow
# autoreconf
# make
# make install
```

Install and configure nfsen

Untar nfsen into the "/opt/" directory.

```
# cd /opt/
# tar -zxvf nfsen-1.3.8.tar.gz
# cd nfsen-nfsen-1.3.8
# cd etc
# cp nfsen-dist.conf nfsen.conf
# vi nfsen.conf
```

Edit the nfsen.conf file with at least the changes below. Make sure all data path variables are set correctly:

```
$BASEDIR= "/data/nfsen";

$HTMLDIR = "/var/www/nfsen"; 'change to' --> $HTMLDIR = "/var/www/html/nfsen";

$PREFIX = '/usr/local/bin'; 'change to' --> '$PREFIX = '/opt/nfdump/bin';

$WWWUSER = "www"; 'change to' --> $WWWUSER = "apache";
$WWWGROUP = "www"; 'change to' --> $WWWGROUP = "apache";
```

Add source for collecting Netflow data from devices:

```
%sources = (
'cisco-router-1' => { 'port' => '9996', 'col' => '#0000ff', 'type' => 'netflow' },
);
```

Run the perl installation script to install nfsen:

```
# cd ..
# ./install.pl etc/nfsen.conf
```

Press enter to accept the default path.

```
Perl to use: [/usr/bin/perl]
```

You may get Errors since we did not configure any flows at this point.

Let's now create a startup script for the service

```
vi /etc/init.d/nfsen
```

Copy the below information into the new configuration file:

```
#!/bin/bash
#! #chkconfig: - 50 50
```

```
#description: nfsen

DAEMON=/data/nfsen/bin/nfsen

case "$1" in
start)
$DAEMON start
;;
stop)
$DAEMON stop
;; status)
$DAEMON status
;;
restart)
$DAEMON stop
sleep 1
$DAEMON start
;;
*)
echo "Usage: $0 {start|stop|status|restart}"
exit 1
;;
esac

exit 0
```

Save the above file.

Make sure the script is executable

```
chmod +x /etc/init.d/nfsen
```

Start the nfsen deamon:

```
/etc/init.d/nfsen start
```

Use the following to restart nfsen when necessary:

```
/etc/init.d/nfsen restart
```

Configure Apache for nfsen web access:

```
# vi /etc/httpd/conf.d/nfsen.conf
```

```
# Add the following line

Alias /nfsen /var/www/html/nfsen/
```

```
<Directory /var/www/html/nfsen/>
DirectoryIndex nfsen.php
 Order Deny,Allow
   Allow from all
</Directory>
```

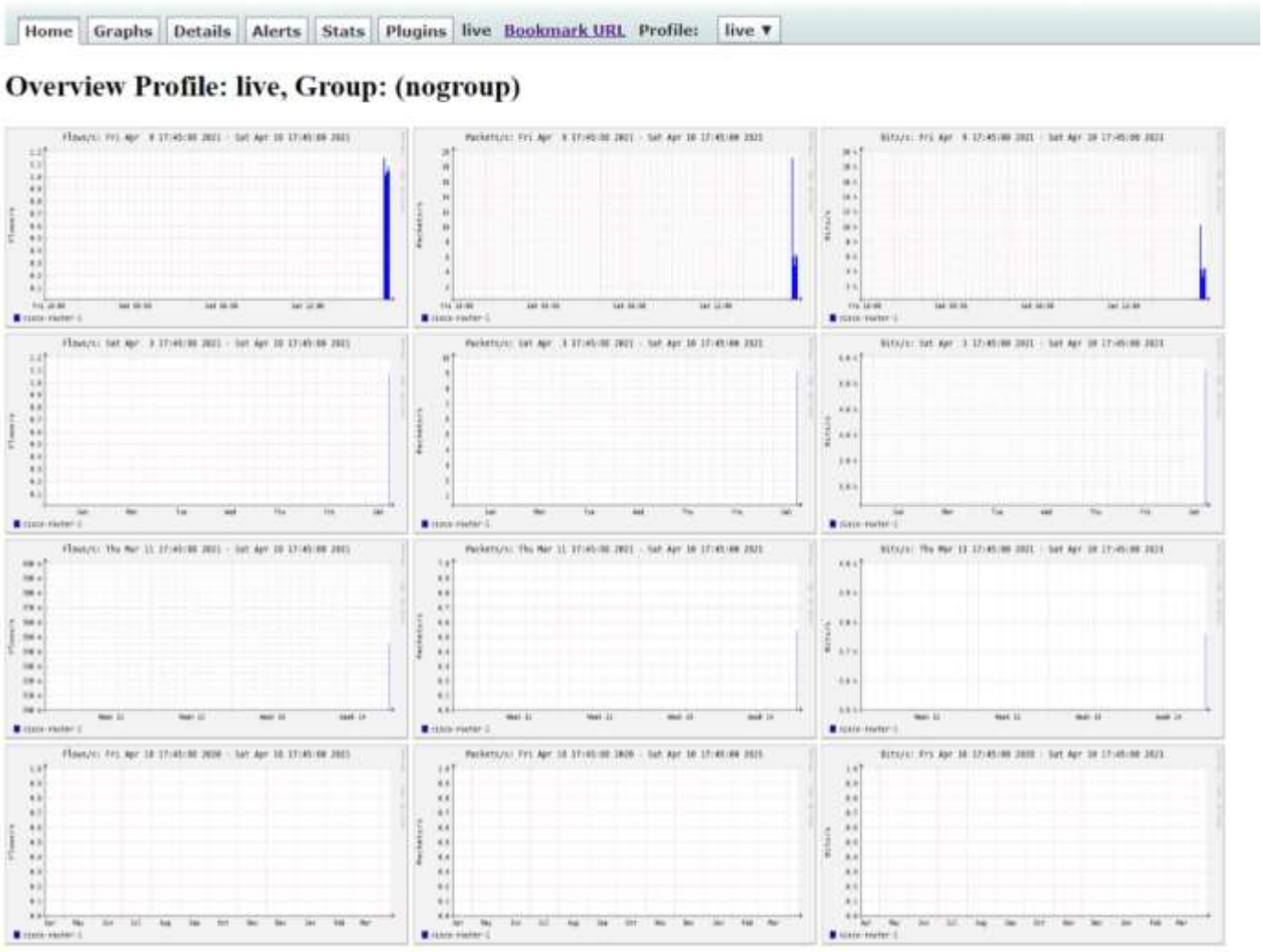
```
# service httpd restart
```

Start the httpd service:

```
service httpd start
```

Now you should be able to access nfsen

Go to **http://your-ip-or-domain/nfsen/nfsen.php**



Configure Netflow on Cisco Router:

```
Cisco-R1#en
Cisco-R1#conf terminal
Cisco-R1(config)#interface  g1/0
Cisco-R1(config-if)#ip route-cache flow
```

```
Cisco-R1(config-if)#exit
Cisco-R1(config)#ip flow-export destination 192.168.20.125 9996
Cisco-R1(config)#ip flow-export source gigabitEthernet 1/0
Cisco-R1(config)#ip flow-export version 5
Cisco-R1(config)#ip flow-cache timeout active 5
Cisco-R1(config)#ip flow-cache timeout inactive 15
Cisco-R1(config)#snmp-server ifindex persist
Cisco-R1(config)#do wr
```

repeat these commands to enable NetFlow for each interface

To see flows:

```
Cisco-R1(config)#do show ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       192.168.20.10 (GigabitEthernet1/0)
    Destination(1)  192.168.20.125 (9996)
  Version 5 flow records
  259 flows exported in 13 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

```
Cisco-R1(config)#do show ip cache flow
IP packet size distribution (4966 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448
  480
   .000 .763 .165 .059 .001 .002 .002 .000 .001 .000 .000 .000 .000 .000 .
  000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .001 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
  5 active, 65531 inactive, 277 added
  5338 ager polls, 0 flow alloc failures
  Active flows timeout in 5 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 533256 bytes
  1 active, 16383 inactive, 263 added, 263 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
```

Turning off NetFlow

If you need to stop exporting NetFlow data from a router, issue the following command in global configuration mode:

```
no ip flow-export destination
```

This will stop exporting the NetFlow cache entries to the specified destination IP address on the specified port number.

If you need to disable NetFlow on an interface, issue the following commands in global configuration mode:

```
interface
no ip route-cache flow
exit
```

Do the following when adding additional NETFLOW Senders:

On the nfsen server, edit the nfsen.conf file to add NetFlow sources:

```
vi /data/nfsen/etc/nfsen.conf
```

You can set the color ('col' => '#xxyyxx') to something you would like by finding a HEX color identifyer at the following site: https://www.color-hex.com/ In place of ("cisco-router-1') and or ('Juniper-router-1') use a friendly name for your device like 'corp-firewall' or 'corp-router'

```
%sources = (
'cisco-router-1' => { 'port' => '9996', 'col' => '#0000ff', 'type' => 'netflow' },
'Mikrotik-router-1' => { 'port' => '9997', 'col' => '#00ffff', 'type' => 'netflow' },
'Fortigate-1' => { 'port' => '9998', 'col' => '#00ffaa', 'type' => 'netflow' },
'Juniper-1' => { 'port' => '9999', 'col' => '#00AAaa', 'type' => 'netflow' },
```

Rebuild NFSEN after all settings changes:

```
# /data/nfsen/bin/nfsen reconfig

# /etc/init.d/nfsen restart
```

Configure NetFlow in Fortigate:

Configuring the Netflow collector IP:

```
#config system netflow

set collector-ip 192.168.20.125
set collector-port 9998
end
```

Enabling Netflow on the Interface:

```
#config system interface
edit port1
```

```
set netflow-sampler both
end
```

Configure NetFlow in MikroTik:

```
#
/ip traffic-flow
set enabled=yes
set interfaces=ether1 or all

/ip traffic-flow target
add dst-address=192.168.20.125 port=9997 version=5
```